[.class="img-fluid clearfix"](#)

`KyberLib` is a Rust-based library that protects your data from the potential threat of quantum computing. Built upon the **CRYSTALS-Kyber algorithm**, `KyberLib` delivers exceptional security, efficiency, and versatility, easily integrating into various platforms, including `no-std` environments.

.class="m-10 w-100"

Securing Your Data in the Quantum Age

The advent of quantum computing has introduced a significant threat to conventional cryptographic security measures. To address this challenge, the field of Quantum-Safe Cryptography (QSC) is swiftly evolving.

At the forefront of this transformative movement is the National Institute of Standards and Technology (NIST), which is spearheading the standardisation of QSC algorithms.

In 2023, NIST shortlisted four innovative algorithms:

- **CRYSTALS-Kyber** ⊡ (key encapsulation mechanism)
- **CRYSTALS-Dilithium** ⊡ (digital signatures)
- **FALCON** ⊡ (lightweight digital signatures)
- **SPHINCS+** ⊡ (hash-based digital signatures)

These groundbreaking algorithms are founded on diverse mathematical principles, including lattice-based cryptography, hash-based cryptography, and code-based cryptography with the aim of providing a robust defence against quantum attacks.

Exploring Lattice-Based Cryptography

Lattice-Based Cryptography (LBC) is emerging as a frontrunner in QSC, offering a promising Post-Quantum Cryptographic (PQC) solution. LBC is versatile, with applications ranging from key-encapsulation mechanisms (KEMs), digital signatures, and public-key encryption schemes rooted in mathematical lattices.

Lattices are a fundamental concept in mathematics that have found applications in various fields, including cryptography. In simple terms, a lattice is a regular arrangement of points in space, forming a grid-like structure. These points are connected by lines, forming a network of interconnected cells. The specific arrangement of points and the spacing between them define the unique characteristics of a lattice.

3D Lattice Representation with Basis Vectors

This graph presents a 3D lattice structure generated by three basis vectors:

- b1 = [1, 0, 0] in red,
- b2 = [0, 1, 0] in green, and
- b3 = [0, 0, 1] in blue.

Each point on the lattice is formed by combining these basis vectors in various integer proportions, creating a grid-like pattern that extends in all three spatial dimensions. The visualisation captures the essence of a 3D lattice, a concept widely used in physics and mathematics to represent the

regular, repeating arrangement of points in space.

3D Lattice Representation with Basis Vectors
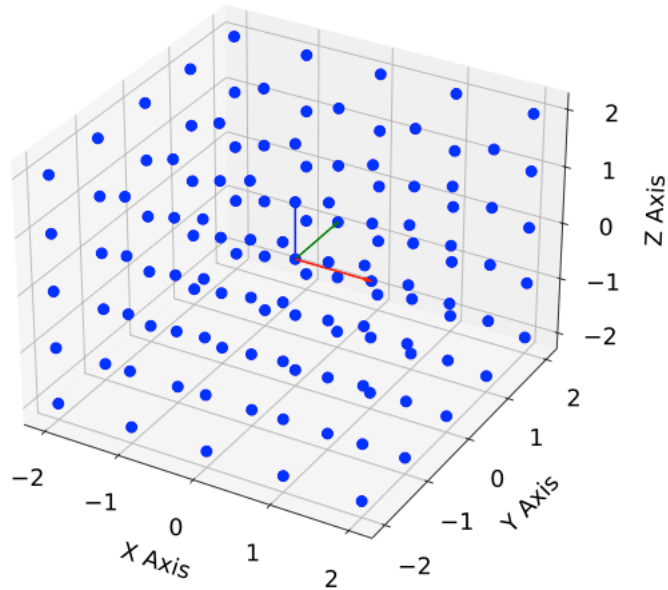
.class="img-fluid mx-

auto d-block"

In cryptography, lattices are employed as the basis for certain cryptographic algorithms. Lattice-Based Cryptography (LBC) exploits the mathematical properties of lattices to create secure cryptographic schemes that are resistant to attacks from quantum computers. Quantum computers pose a significant threat to conventional cryptography, as they can efficiently break algorithms that rely on factoring large numbers or solving discrete logarithm problems.

CRYSTALS-Kyber exemplifies the strengths of LBC, providing robust resistance against quantum attacks coupled with exceptional efficiency and key size. Its multiple platforms and compatibility with cryptography make it a reliable quantum-era data security option.

The CRYSTALS-Kyber current specifications are as follows:

- **Kyber512**: Provides a security level equivalent to 128-bit AES encryption, safeguarding sensitive data with industry-standard protection.
- **Kyber768**: Provides a security level equivalent to 256-bit AES encryption, ensuring the confidentiality of highly sensitive information.
- **Kyber1024**: Provides a security level exceeding 256-bit AES encryption, offering robust protection against quantum attacks and safeguarding data integrity far into the future.

Comparison of Security Levels between Classical and Quantum-Resistant Algorithms

This bar chart illustrates the relative security levels of classical cryptographic algorithms like RSA-2048 and Elliptic Curve Digital Signature Algorithm (ECDSA) compared to the specifications of quantum-resistant CRYSTALS-Kyber Algorithm variants (Kyber512, Kyber768, and Kyber1024).

While the chart provides a visual comparison, it's crucial to note that the security levels aren't directly comparable due to their foundation on different mathematical principles.

However, the chart does provide a useful reference point for understanding the security levels of quantum-resistant algorithms.

Comparison of Security Levels between Classical and Quantum-Resistant Algorithms
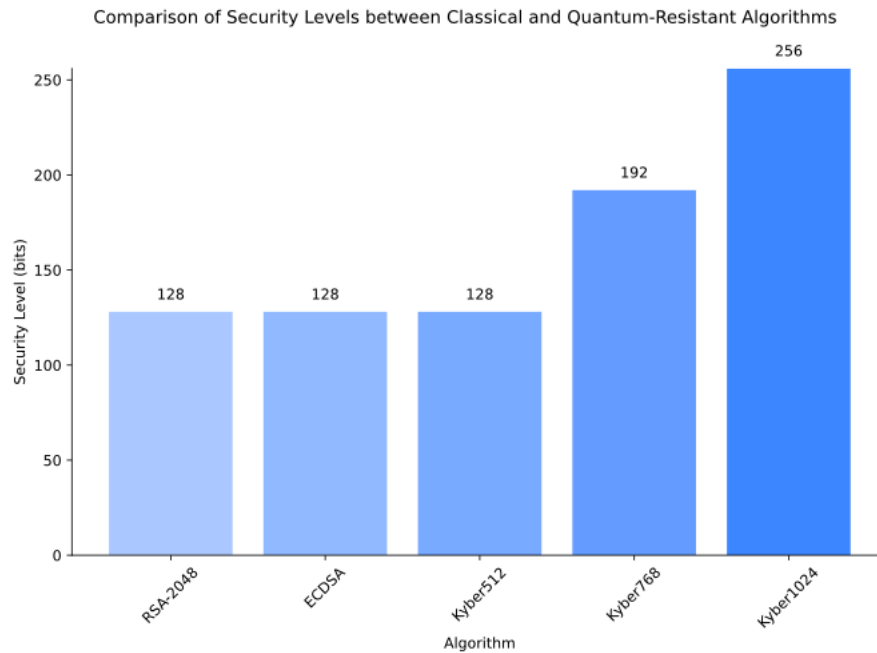
.class="img-fluid mx-auto d-block"

.class="m-10 w-100"

KyberLib: A Rust Library for Quantum-Resistant Cryptography

KyberLib harnesses the power of CRYSTALS-Kyber to deliver enhanced memory safety and robust system-level security. It supports multiple CRYSTALS-Kyber specifications (Kyber512, Kyber768, Kyber1024), offering a range of security levels to suit your specific needs. Its `no_std` compliance makes it an ideal choice for embedded systems, while its WebAssembly (WASM) compatibility facilitates seamless integration into web applications.

.class="m-10 w-100"

Protecting Web Applications With Quantum-Resistant Cryptography

Designed for a minimal memory footprint, KyberLib is ideal for embedded and resource-limited systems without compromising security. Its Rust-based implementation capitalises on the language's safety features, fortifying the security offered by the CRYSTALS-Kyber algorithm.

Additionally, KyberLib's WebAssembly compatibility enhances its utility in web applications, guaranteeing that it remains a vital tool in the dynamic realm of cryptography.

[Get Started with KyberLib Now!](#) ⧉ Effortless to install, free for both personal and commercial use, KyberLib is your go-to solution for quantum-resistant cryptography.